

REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Information Disclosure Statement

The Applicant respectfully requests that the Examiner indicate that the references cited in the Information Disclosure Statement filed on December 4, 2003 have been reviewed by returning an initialed copy of the PTO-1449 Form.

Disposition of the Claims

Claims 1-8, 10-16, 18-23, and 25-37 are pending in the present application. Claims 1, 18, 28, 29, 35, 36, and 37 are independent. The remaining claims depend, directly or indirectly, from claims 1, 18, and 29.

Claim Amendments

Claims 1, 18, 28, 29, 35, 36, and 37 have been amended by way of this reply to include the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication.” Support for these amendments may be found in at least paragraphs [0034] and [0035]. No new subject matter has been added by way of these amendments.

Rejections under 35 U.S.C. § 103

Claims 1, 2, 5, 7, 11-13, 18-20, 26, 29-32, 36, and 37

Claims 1, 2, 5, 7, 11-13, 18-20, 26, 29-32, 36, and 37 are rejected under 35 U.S.C. § 103(a) as being unpatentable over EP 0820207 A2 (hereinafter referred to as “Lipsit”) in view of U.S. Patent Application Publication No. 2002/0034940 (“Takae”) in further view of U.S. Patent No. 6,542,729 (“Chmaytelli”). To the extent this rejection applies to the amended claims, this rejection is respectfully traversed.

The claimed invention relates to unblocking a security device that issued to an end user. A security device corresponds to a component that provides strong end user authentication. Strong end user authentication is an authentication technique that permits entities to provide evidence that they know a particular secret without revealing the secret. (*See, e.g.*, paragraph [0035] of the Instant Specification). Specifically, a security device is accessed by a security device reader that is connected to a computer system. The security device may be blocked, for example, when an end user enters a personal information number (PIN) too many times. When the security device is blocked, a security agent is contacted and given information about the end user and security device. As disclosed in at least one embodiment of the invention, the security agent (using the Schlumberger Smart Port (SSP)) verifies the end user exists and is the user assigned the particular security device while the end user is in possession of the security device. (*See, e.g.*, paragraphs [0038], [0048] and [0049] of the Instant Specification). Only after the security agent has verified that the end user exists and is assigned the particular security device in the end user's possession, is an unblock authorization code (UAC) generated. (*See, e.g.*, paragraph [0050] of the Instant Specification). The UAC may then be used by the client side transfer agent to query an unblocking service and obtain an Unblock Code (UBC) that is used to unblock the security device. Accordingly, the invention as recited in the claims requires, in part, that the security device being unblocked using the above technique is configured to be accessed by a security device reader to allow access to a computer system to provide strong end user authentication. In other words, a security device and a security device reader, which is configured to allow access to a computer system, are all required elements.

Turning to the rejection, to establish a prima facie case of obviousness "...the prior art reference (or references when combined) must teach or suggest all the claim limitations." (*See* MPEP §2143.03). Further, "***all words*** in a claim must be considered in judging the patentability of that claim against the prior art." (*See* MPEP §2143.03 [emphasis added]). The Applicant respectfully asserts that the references, when combined, fail to teach or suggest all the claim limitations of the amended claims.

The Examiner contends that Lipsit describes a system in which a secure gateway is used to coordinate unblocking of a security device (Office Action dated March 29, 2006 at page 3). In

essence, Lipsit relates to activating a cell phone by authorizing a user to access the cell phone network.

Applicant respectfully asserts that Lipsit does not teach or suggest a security device, which is “configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication,” as recited in the amended claim 1. Simply put, the cell phone taught in Lipsit is not configured to be accessed by a security device reader (connected to a computer system) allowing access to the computer system to perform strong end user authentication.

Initially, within the added limitation, claim 1 requires three separate components, namely (1) a security device (as described in paragraph [0035] in the specification), (2) a security device reader (*e.g.*, card reader (50) as shown in Figure 2 and described in paragraph [0034] in the specification), and (3) a computer system (*e.g.*, computer (40) as shown in Figure 2 and described in paragraph [0034] in the specification). No matter how broadly the cell phone in Lipsit is read, Applicant contends these three components are not taught or suggested in Lipsit.

Further, to assert that the system in Lipsit teaches the configuration recited in the amended claim 1, the Examiner would be required to mischaracterize Lipsit. Specifically, even assuming, *arguendo*, that a cell phone is a security device (or even contains a security device), the cell phone (or chip within the cell phone) is not configured to be accessed by a security device reader, as contemplated in the recited claim.

Additionally, even assuming, *arguendo*, that the cell phone is somehow accessed by a security device, Lipsit does not even come close to teaching a security device reader connected to and allowing access to a computer system to provide strong end user authentication. As shown in Figure 2 of the instant specification, the security device reader (*e.g.*, card reader (50)) is connected to a computer system (*e.g.*, computer (40)), which accepts and accesses a security device (*e.g.*, a card inserted into a slot in the card reader (50)). No matter how broadly the Examiner reads Lipsit, such a configuration is not contemplated or taught in Lipsit.

Next, access to the computer system (*e.g.*, computer (40) in Figure 2) is allowed to provide strong end user authentication. As clearly supported in the specification, strong end user

authentication is “an authentication technique that permits entitles to provide evidence that they know a particular secret without revealing the secret” (Instant Specification at [0035]). Applicant asserts that Lipsit fails to teach or suggest strong end user authentication, as recited in the claims. As it is widely known, a cell phone number can be easily hijacked without the cell phone by various nefarious individuals and used to make calls. Even the phone network used to transmit the calls and any entity at the other end of the calls would not be able to differentiate between the various nefarious individuals and the actual owner of the cell phone. Applicant argues that, when using the authentication technique described in Lipsit, the “secret” is known by everyone involved. Specifically, the cell phone user is provided the security code and that *same* security code is stored in a database and used by the Activation Unit to provide authorization to the user (See, Lipsit at pp. 5, ll. 42-60 – 6, ll.1-17). Additionally, the serial number of the cell phone, which may also be used during activation, is also available for everyone to see. Thus, the cell phone and cell phone network taught in Lipsit could not be considered to teach or suggest strong end user authentication.

In view of the above, Lipsit fails to teach or suggest the limitations recited in amended claim 1.

Further, Applicant asserts Takae fails to teach that which Lipsit lacks, as evidenced by the fact that the Examiner relies on Takae solely to teach “verification while an end user is in possession of the device” (See Office Action dated March 29, 2006 at page 3). Further, Takae merely teaches upgrading a cell phone. (See, *e.g.*, Takae, abstract, Figures 1 and 2). Takae does not even mention or contemplate a security device or security device reader.

In view of the above, Takae and Lipsit, whether considered together or separately, fail to teach or suggest each and every limitation of amended claim 1.

Further, Applicant asserts Chmaytelli fails to teach that which Lipsit and Takae lack as evidenced by the fact that the Examiner relies on Chmaytelli solely to teach “that a device may be physically locked and an unblock code may be sent to a device to unblock the code to the device” (See Office Action dated March 29, 2006 at page 3).

In view of the above, Chmaytelli, Takae, and Lipsit, whether considered together or separately, fail to teach or suggest each and every limitation of amended claim 1.

Moreover, the Examiner's purported rationale for modifying Lipsit with the teachings of Chmaytelli does not comply with the requirements for establishing a motivation to combine the references. Specifically, MPEP §2143.01 states that "the mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." Citing *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990).

The portion of Lipsit relied upon by the Examiner to teach the limitation "an Unblock authorization code generated after verification by the security agent and securely transferred from the agent-side transfer agent to the unblocking service, wherein verification comprises verifying the end user is assigned the security device" merely teaches verifying that an end user *can* purchase a cell phone by checking the billing and credit information of the end user before the end user has possession of the cell phone (*See, e.g.*, Lipsit p. 5 ll. 42-50). Chmaytelli teaches unlocking the cell phone when fraudulent usage has occurred (*See, e.g.*, Chmaytelli Abstract). When an end user has not yet purchased a cell phone as required in Lipsit, there is no reason for the end user to want to unlock the cell phone because of fraudulent usage as taught in Chmaytelli. Specifically, an end user that physically has the cell phone does not need to be verified that they can purchase the cell phone. Accordingly, one skilled in the art would have absolutely no reason to combine the references.

Even assuming *arguendo* that an end user that has not yet bought a cell phone would want to unlock the cell phone, a motivation to combine the security code (*i.e.*, what the Examiner equates to the Unblock Authorization Code) of Lipsit and the code to enter into the mobile telephone (*i.e.*, the Unblock Code) of Chmaytelli does not exist. Specifically, both codes are obtained from either a salesperson or an operator. There is no reason that is presented in either reference for the end user to contact the salesperson with one code to give to the operator to get another code to unblock the mobile telephone. In fact, such modification would require an unnecessary extra step for the end user and therefore would be contrary to any desire to make the modifications. Again, one skilled in the art would have absolutely no reason to combine the references.

Thus, the Examiner rationale supporting his assertion that it would have been obvious to modify Lipsit with Chmaytelli is not sufficient because he has not shown specifically where in the prior art a suggestion is found regarding the desirability of such modification. Accordingly, if the Examiner wishes to maintain this rejection, the Applicant respectfully requests that the Examiner indicate where in Lipsit or Chmaytelli there is support for the desirability of making the modification suggested by the Examiner. If such support cannot be provided, then the Applicant respectfully requests the Examiner to withdraw the rejection because the Examiner has not satisfied the requirements for establishing a motivation to combine Lipsit and Chmaytelli.

In view of the above, Lipsit, Takae, and Chmaytelli, whether considered together or separately, do not support the rejection of amended independent claim 1. Independent claims 18, 29, 36, and 37 have also been amended to include substantially the same limitations as amended claim 1 and are allowable for at least the same reasons. Dependent claims 2, 5, 7, 11-13, 19, 20, 26, and 30-32, which depend directly or indirectly on claims 1, 18, and 29, are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 3, 4, 22, and 23

Claims 3, 4, 22, and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Menezes, Alfred J. Handbook of Applied Cryptography (hereinafter referred to as “Menezes”). Claims 3, 4, 22, and 23 depend on amended independent claim 1 or 18. To the extent this rejection still applies to the amended claims, this rejection is respectfully traversed.

As discussed above, Lipsit, Takae and Chmaytelli fail to teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication” found in claims 1 and 18. Further, Menezes does not teach that which Lipsit, Chmaytelli, and Takae lack as evidenced by the fact that the Examiner relies on Menezes solely to teach “the idea that a password is typically presented with an end user identifier as an end user identifier/password pair” (See Office Action dated March 29, 2006 at page 6).

In view of the above, Lipsit, Takae, Chmaytelli, and Menezes, whether considered together or separately, do not support the rejection of amended independent claims 1 and 18. Dependent claims 3, 4, 22, and 23, which depend on claims 1 and 18, are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 6 and 21

Claims 6 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of U.S. Patent Application Publication No. 2002/0112156 (hereinafter referred to as “Gien”). Claims 6 and 21 are dependent on amended independent claims 1 and 18, respectively. To the extent this rejection still applies to the amended claims, this rejection is respectfully traversed.

As discussed above, Lipsit, Takae, and Chmaytelli fail to teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication” found in claims 1 and 18. Further, Gien does not teach that which Lipsit, Takae, and Chmaytelli lack as evidenced by the fact that the Examiner relies on Gien solely to teach “the idea of unblocking a smart card” (See Office Action dated March 29, 2006 at page 7).

Moreover, Applicant respectfully asserts that there is no motivation to combine Gien with Lipsit, Takae, and Chmaytelli. Specifically, in order to protect the contents of the Smart Card, Gien explicitly states that when the smart card is blocked in a reversible state only the entity that issues the smart card can unblock it. If it is permanently blocked, then the smart card is completely inaccessible. (*See, e.g.*, Gien paragraph [0110]-[0113]) Because Gien explicitly states that only the entity that issues the smart card can unblock the smart card for security reasons, Gien clearly teaches away from having a client-side transfer agent perform the orchestration of unblocking the smart card by obtaining the unblock code from the unblocking service. Specifically, in Gien, the client is not trusted to perform such functions. Accordingly, the Applicant respectfully requests the Examiner to withdraw the rejection because the Examiner has not satisfied the requirements for establishing a motivation to combine Gien with Lipsit, Takae, and Chmaytelli.

In view of the above, Lipsit, Takae, Chmaytelli, and Gien, whether considered together or separately, do not support the rejection of amended independent claims 1 and 18. Dependent claims 6 and 21, which depend on claims 1 and 18, are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 10 and 25

Claims 10 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of U.S. Patent Application Publication No. 2002/0138553 (hereinafter referred to as “Binder”). Claims 10 and 25 are dependent on amended independent claims 1 and 18, respectively. To the extent this rejection still applies to the amended claims, this rejection is respectfully traversed.

As discussed above, Lipsit, Takae, and Chmaytelli fail to teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication” found in claims 1 and 18. Further, Binder does not teach that which Lipsit, Takae, and Chmaytelli lack as evidenced by the fact that the Examiner relies on Binder solely to teach “the idea checking at a configurable frequency for the UAC for a generated message” (See Office Action dated March 29, 2006 at page 8).

In view of the above, Lipsit, Takae, Chmaytelli, and Binder, whether considered together or separately, do not support the rejection of amended independent claims 1 and 18. Dependent claims 10 and 25, which depend on claims 1 and 18, are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 8, 14-16, and 27

Claims 8, 14-16 and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Menezes. Claims 8, 14-16, and 27 are dependent on amended independent claims 1 and 18. To the extent this rejection still applies to the amended claims, this rejection is respectfully traversed.

As discussed above, Lipsit, Takae, Chmaytelli, and Menezes fail to teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication” found in claims 1 and 18. Dependent claims 8, 14-16, and 27, which depend on claims 1 and 18, are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 28

Amended independent claim 28 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Binder. To the extent this rejection still applies to amended independent claim 28, this rejection is respectfully traversed.

As discussed above, Lipsit, Takae, Chmaytelli, and Binder fail to teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication” found in amended independent claim 28. Accordingly, in view of the above, Lipsit, Takae, Chmaytelli, and Binder, whether considered together or separately, do not support the rejection of amended independent claim 28. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 33

Claim 33 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of U.S. Patent Application Publication No. 2003/0013434 (hereinafter referred to as “Rosenberg”). Claim 33 is dependent on amended independent claim 29. To the extent this rejection still applies, this rejection is respectfully traversed.

As discussed above, Lipsit, Takae, and Chmaytelli fail to teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication”

found in claim 29. Further, Rosenberg does not teach that which Lipsit, Takae, and Chmaytelli lack as evidenced by the fact that the Examiner relies on Rosenberg solely to teach “the idea of generating a UBC (activation code) for a user and delivering the new UBC to a directory service where it can be obtained by the user” (See Office Action dated March 29, 2006 at page 11).

In view of the above, Lipsit, Takae, Chmaytelli, and Rosenberg, whether considered together or separately, do not support the rejection of amended independent claim 29. Dependent claim 33, which depends on claim 29, is allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 34

Claim 34 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of U.S. Patent No. 5,949,882 (hereinafter referred to as “Angelo”). Claim 34 is dependent on amended independent claim 29. To the extent this rejection still applies to the amended claims, this rejection is respectfully traversed.

As discussed above, Lipsit, Takae, and Chmaytelli fail to teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication” found in amended claim 29. Further, Angelo does not teach that which Lipsit, Takae, and Chmaytelli lack as evidenced by the fact that the Examiner relies on Angelo solely to teach “the idea of making a check on a security device to make sure it is not permanently blocked” (See Office Action dated March 29, 2006 at page 12).

In view of the above, Lipsit, Takae, Chmaytelli, and Angelo, whether considered together or separately, do not support the rejection of amended independent claim 29. Dependent claim 34 which depends on claim 29 is allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 35

Amended independent claim 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of

Rosenberg in further view of Angelo. To the extent this rejection still applies to amended claim 35, this rejection is respectfully traversed.

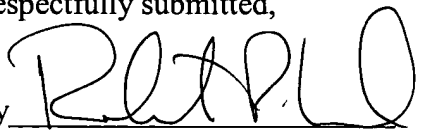
As discussed above, Lipsit, Takae, Chmaytelli, Rosenberg, and Angelo, whether considered together or separately, do not teach or suggest the limitation “wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication” found in amended independent claim 35. Accordingly, Lipsit, Takae, Chmaytelli, Rosenberg, and Angelo, whether considered together or separately, do not support the rejection of amended independent claim 35. Withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09469/007001).

Dated: June 29, 2006

Respectfully submitted,

By 

Robert P. Lord
Registration No.: 46,479
OSHA • LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant